NASED Independent Test Authority Qualification Testing

Carolyn Coggins, Director of ITA Services
Gail Audette, Vice-President of Engineering and Chief Operating Officer
SysTest Labs, LLC
216 16th St., 7th Floor, Denver, Co 80202

SysTest Labs is pleased to provide the Environment, Technology, and Standards Subcommittee with information about ITA (Independent Testing Authority) Qualification Testing of Voting Systems for the National Association of State Election Directors (NASED) to the Federal Election Commission (FEC) Voting System Standards (VSS).

Three labs currently provide NASED Qualification Testing. All of the labs test to the VSS, but each has their own methods. Our comments here reflect the methods used by SysTest Labs.

My discussion shall identify:

- SysTest Labs' qualifications and accreditation as an ITA;
- The standards, in addition to the VSS, that govern qualification testing;
- How the Voting System Qualification Test process is defined in the VSS;
- How SysTest Labs implements the VSS Voting System Qualification Test process;
- How SysTest Labs maintains quality and manage process improvement; and
- Observations and recommendations regarding lab accreditation, the VSS and qualification testing.

Accreditation as a NASED Qualification ITA

SysTest Labs' is full service laboratory specializing in all areas of software testing. Our work ranges from Independent Verification and Validation for software development efforts of state unemployment insurance systems to large and complex software laboratory testing for major telecommunication companies to web site performance testing for major retailers to software test staff augmentation. SysTest Labs has successfully completed over 500 software testing or quality assurance projects for over 250 clients worldwide. Regardless of the test effort, all aspects of our quality program, test methodology and test engineer training are guided by Institute of Electrical and Electronic Engineers (IEEE) standards and the SysTest Labs quality procedures.

In order to become a software and hardware ITA, SysTest Labs had to apply to NASED and then be audited by the NASED Technical Committee. To my knowledge, we are the only lab that has sought and been awarded both software and hardware accreditation, to become a full service ITA. We initially applied and qualified as a software ITA in 2001. We recently granted acceptance as a hardware ITA. Our hardware ITA status is provisional, i.e. our audit was successfully completed, NASED has recommended accreditation and our initial hardware qualification test effort will be monitored by a NASED auditor.

Quality Program, Test Standards and Test Methods

The NASED audit process requires that we provide documentation and demonstrate our quality program. In addition, we have had to provide documentation and demonstrate our test methodology and processes for NASED Qualification Testing of voting systems. While the requirements we test to are governed by the standards, we must define the method of testing and processes to ensure the consistency, adequacy, accuracy, and overall quality of our NASED Qualification Testing.

While the 2002 Federal Election Commission Voting System Standard is the primary standard, there are a number of other standards used in our voting system testing. The VSS itself incorporates a number of other standards, which are included in NASED Qualification Testing (see Volume 1 Applicable Documents). The primary standards we use in NASED ITA Qualification Testing are:

Federal Election Commission

- Federal Election Commission Voting System Standards, Volume I Performance Standards and Volume II Test Standards, April 2002.

National Association of State Election Directors

- NASED Accreditation of Independent Testing Authorities for Voting System Qualification Testing, NASED Program Handbook NHDBK 9201, a National Association of State Election Directors (NASED), May 1st, 1992.
- NASED Voting System Standards Board Technical Guide #1, FEC VSS Volume I, Section 2.2.7.2, Color and Contrast Adjustment
- NASED Voting System Standards Board Technical Guide #2, Clarification of Requirements and Test Criteria for Multilanguage Ballot Displays and Accessibility

Institute of Electrical and Electronics Engineers

- IEEE Standard for Software Quality Assurance Plans IEEE STD 730-1998
- IEEE Standard for Software Configuration Management Plans IEEE STD 828-1998,
- IEEE Standard for Software Test Documentation IEEE STD 829-1998
- IEEE Recommended Practice for Software Requirements Specifications IEEE STD 830-1998
- IEEE Standard for Software Unit Testing IEEE STD 1008-1987
- IEEE Standard for Software Verification and Validation IEEE Std 1012-1998.

Federal Regulations

- Code of Federal Regulations, Title 20, Part 1910, Occupational Safety and Health Act
- Code of Federal Regulations, Title 36, Part 1194, Architectural and Transportation Barriers Compliance Board, Electronic and Information Technology Standards - Final Rule
- Code of Federal Regulations, Title 47, Parts 15 and 18, Rules and Regulations of the Federal Communications Commission
- Code of Federal Regulations, Title 47, Part 15, "Radio Frequency Devices", Subpart J, "Computing Devices", Rules and Regulations of the Federal Communications Commission

American National Standards Institute

- ANSI C63.4 Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9Khz to 40 GHz

- ANSI C63.19 American National Standard for Methods of Measurement of Compatibility between Wireless Communication Devices and Hearing Aids

International Electrotechnical Commission

Electromagnetic Compatibility (EMC) Part 4: Testing and Measurement Techniques

- IEC 61000-4-2 (1995-01) Section 2 Electrostatic Discharge Immunity Test (Basic EMC publication)
- IEC 61000-4-3 (1996) Section 3 Radiated Radio-Frequency Electromagnetic Field Immunity Test
- IEC 61000-4-4 (1995-01) Section 4 Electrical Fast Transient/Burst Immunity Test
- IEC 61000-4-5 (1995-02) Section 5 Surge Immunity Test
- IEC 61000-4-6 (1996-04) Section 6 Immunity to Conducted Disturbances Induced by Radio-Frequency Fields
- IEC 61000-4-8 (1993-06) Section 8 Power-Frequency Magnetic Field Immunity Test. (Basic EMC publication)
- IEC 61000-4-11 (1994-06) Section 11. Voltage Dips, Short Interruptions and Voltage Variations Immunity Tests

Electromagnetic compatibility (EMC) Part 5-7: Installation and mitigation guidelines

- IEC 61000-5-7 Ed. 1.0 b: 2001 Degrees of protection provided by enclosures against electromagnetic disturbances

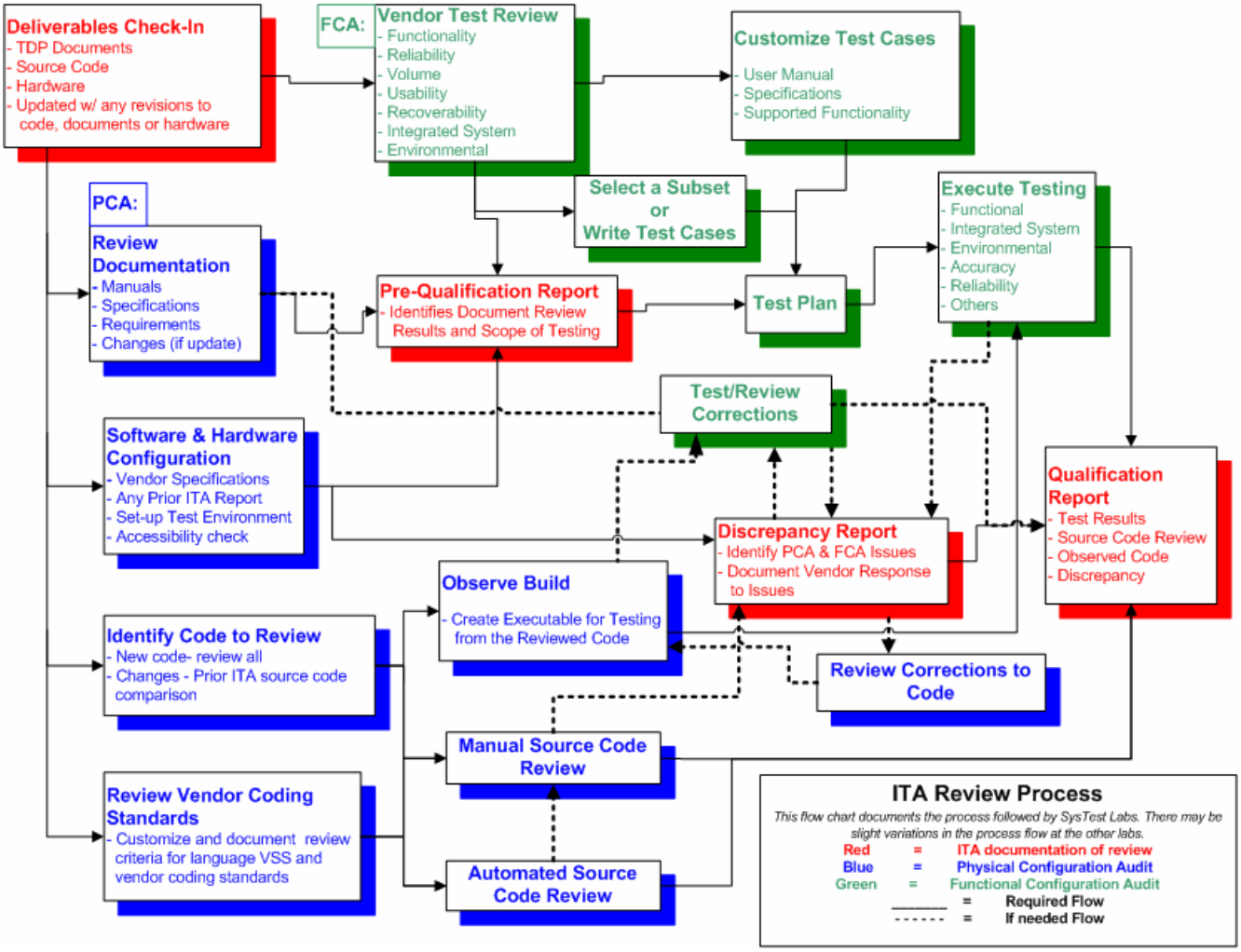
Military Standards

- MIL-STD-810D (2) Environmental Test Methods and Engineering Guidelines

NASED Qualification Testing of Voting Systems ITA Process

SysTest Labs performs qualification testing in conformance with the two processes required in the 2002 VSS. The results from Qualification reviews and testing are documented throughout the process (ITA documentation of testing in red):

- Physical Configuration Audit (PCA in blue) addresses the physical aspects of the voting system, including:
  - Review of the Technical Data Package (TDP) documentation
  - Verification of the configuration of the hardware and software
  - Identification of the code to review
  - Source Code review
  - Observing the building of the executable from the reviewed source code
- Functional Configuration Audit (FCA in green) addresses the functional aspects of the voting system, including:
  - Review of all testing performed by the vendor
  - Test planning
  - Test Case preparation and/or customization of Standard Test Cases
  - Test execution



While the VSS outlines the overall PCA and FCA process, SysTest Labs has defined specific processes for each area of testing or review to ensure a consistent, repeatable test methodology. These processes include specific review and test templates that have been prepared in conformance with the VSS, IEEE standards, NASED accreditation policies and SysTest Labs quality procedures. Each voting system is unique. While qualification testing must be customized for the unique requirements of each specific voting system, the overall process is exactly the same for every voting system.

The VSS does not designate software and hardware ITA responsibilities. These responsibilities are assigned by NASED accreditation policies. The processes documented here note processes or test approaches that can be applied to either the software or hardware ITA.

- **PCA Technical Data Package (TDP) Review:** The TDP is reviewed to confirm required documentation is present, conforms in content/format and is sufficient to install, validate, operate, maintain the voting system and establish the system hardware baseline associated with the software baseline. Results of the review are provided to the vendor in a Pre-qualification Report.
- **PCA Source Code Review:** The source code is reviewed for:
    - Maintainability – including the naming, coding and comment conventions, adherence to coding standards and clear commenting.

  - Control Constructs – to determine the logic flow utilizes standard constructions of the development language, its used consistently, the logic structure isn't overly complex and there's an acceptable use of error handlers. Where possible automated tools are used.
  - Modularity – confirming each module has a testable single function, unique name, single entry/exit, contains error handling and an acceptable module size.
  - Security and Integrity of the Code – including controls to prevent deliberate or accidental attempts to replace code such as unbounded arrays or strings, including buffers to more data, pointer variables and dynamic memory allocation and management; and other security risks, such as hard coded passwords.
- **PCA Test Environment:** The Hardware and Software ITAs document the setup of the voting system configuration to assure a consistent test environment. The ITAs observe building of the executable from reviewed source code. The Hardware and Software ITAs work together to confirm that all testing is performed only on ITA reviewed code built under ITA observation.
- **FCA Test Documentation Review:** The ITA reviews and assesses prior testing performed by the vendor. Based upon the assessment of vendor testing the ITA identifies scope; designs testing; and creates the Qualification Test Plan.
- **FCA Testing:** Each ITA tests to their identified scope, using their own internal processes.
  - **Polling Place System Testing**: The Hardware ITA initiates environmental operating and non-operating tests; functional testing of polling place hardware/software, and user manuals for all VSS-required and optional vendor supported functionality; testing the capability of the voting system to assist voters with disabilities or language; and accuracy and reliability testing.
  - **Election Management System Testing**: The Software ITA initiates functional testing of the Ballot Preparation and Central Count hardware/software, and user manuals for all VSS-required and optional vendor supported functionality.
  - **System Level Testing**: The Software ITA initiates end-to-end testing of the integrated EMS and Polling Place System, including testing of the system capabilities and safeguards, claimed by the vendor in its TDP.

Creating the Test Methodology and Maintaining Quality

In structuring our review and test methodology we are guided by a continual quest to improve the process and quality. From the foundation of our first ITA project we have continually examined our methods. Through ten completed or active projects we have honed and revised our processes. Some changes have been based upon internal 'lessons learned' and others have come from the external changes in the ITA process, such as the update to the 2002 VSS.

The process we followed in creating and maintaining the NASED Qualification Testing was to define and document a review and test process for both management and test activities. This process needed to be standardized, repeatable and integrated into the overall structure for all SysTest Labs testing projects. Within this standard structure we tailored the individual methods to the unique requirements of software ITA qualification testing based upon the 1990 VSS. Processes addressed in this phase included VSS requirements management, test elements (plans, test cases, reviews and reports), test management, defect tracking, basic training, quality assurance, configuration management (vendor materials and our testing) and project management.

Our next step was to work with and observe and improve the process through successive test efforts. In this phase we broadened our view to training needs, organizational coordination of the individual test tasks and peer reviews. With each effort we reworked some processes and identified other areas for potential process improvement.

At the point the 2002 VSS was implemented, we had a solid structure and the perfect opportunity to implement several identified process improvements, in conjunction with a conversion to the new standards.

While we continue to observe our processes, we are also moving into an optimization phase. In our expanded role as a hardware ITA we will be initiating some new processes that will follow our historic model, but will also look at some of our old processes and optimize them for an increased workload.

Observations and Recommendations for Lab Accreditation

The majority of VSS requirements for qualification testing involve software. There are unique environmental tests that address hardware specifically, but the VSS requires that a portion of software testing for accuracy and reliability be performed in environmental chambers. In doing so there is an overlap. The most effective way to handle this overlap is to create a structure that permits joint testing of the hardware and software. NASED structured the scope of testing so that the hardware ITA was responsible for functional software and hardware testing on the polling place equipment and environmental testing of the hardware. The software ITA has been responsible for the ballot preparation and central count functionality along with integration testing of the entire system (end-to-end elections processes). While the software ITA does not review all the code, they must receive all of the code in order to perform end-to-end testing on the integrated system.

We feel this scope should be changed due to the following issues:

- Polling place software cannot be fully tested without integrating the entire voting system. Today's new voting system vendors do not develop separate applications. In the majority of systems we see, a vendor is forced to artificially divide their code in order to give the polling place software to the hardware ITA and the balance to the software ITA.
- The ITA labs try to keep duplication of effort down to a minimum, however integration testing must repeat much of the polling place functional testing.
- Vendors are required to return to the hardware ITA for regression testing if issues are uncovered during integration testing. If the software ITA uncovers an issue in the polling place during integration testing, they must notify the hardware ITA. While the software ITA must rerun their tests with the new version of the code, the hardware ITA is responsible for reviewing the code changes to fix the issue and functionally testing to confirm the fix. In addition, there have been times when ITA labs have an inconsistent interpretation of the standards and a vendor's solution will overlap between the hardware and software ITA.
- While environmental hardware testing requires specialized equipment and testing, the environmental test methodology is not unique to voting systems and generally does not require specialized knowledge of voting. Furthermore, effective software testing does require specialized knowledge of voting practices.

We recommend that accreditation of labs include the following:

- Primary labs that bear responsibility for all testing, review and reporting. Primary labs may have qualified subcontractors to perform specialized testing, e.g., hardware environmental testing. The primary lab must demonstrate their ability to monitor the work of the subcontractors and verify that all subcontractor work reflects quality processes equal to or greater than those of the primary lab;
- Validation of an understanding of the unique functional requirements of voting systems and voting system standards;
- Validation of manual and automated software testing experience, methodology and software quality engineering practices meet a minimum of CMMI Level 3; and
- Validation of test equipment and chambers sufficient to perform all VSS defined environmental testing, as well as environmental testing experience, methodology and quality engineering practices.

Observations and Recommendations for Voting System Standards

One hears much discussion on the adequacy of the 2002 FEC Voting System Standards with extensive criticism against the adequacy of security standards, but perhaps these critics are not taking a broad view of how the VSS addresses security. Basic functionality requirements, such as printing the name of an election and date on all reports, are an aspect of security. Voting system, accuracy and reliability are aspects of securing the vote. Any functional requirement of the VSS that deals with election creation, voting, counting or auditing is an aspect of securing the vote. The VSS requirement for a vendor to identify the weight of paper deals with the security of the vote. Additionally, the VSS requirements call for documentation of the process to ensure physical security of a voting system and the ability to detect intrusion. When looked at from this broad view, the requirements of the VSS are quite comprehensive.

Criticism is generally is focused on the narrower view of security in terms of active attack code such as viruses, worms, Trojan horses, logic bombs, backdoors, exploitable vulnerabilities, and programming flaws. The VSS provides some detail here. There are also sections in the VSS that provide the labs with some wider latitude. In Volume 2 Section 1.5 the VSS states *"Additionally, new threats may be identified that are not directly addressed by the Standards or the system. As new threats to a voting system are discovered, either during the system's operation or during the operation of other computer-based systems that use technologies comparable to those of another voting system, ITAs shall expand the tests used for system security to address the threats that are applicable to a particular design of voting system.*" A statement like this allows the individual lab a great deal of discretion in testing. What it does not do is provide the detail for consistency across all ITA testing.

Is providing more detail being addressed? HAVA specifically identifies a review of the security and accessibility requirements of the VSS and creation of new voting standards by the EAC, with the support of NIST.

Is there anything that can be done to enhance the VSS without waiting for the writing of new standards? Yes. The 2002 FEC Voting System Standards Implementation Plan identified a process for issuing clarification bulletins. This year NASED Voting System Standards Board Technical Guides 1 and 2 were issued with clarifications of two VSS requirements dealing with accessibility. Although NASED

has a mechanism to issue clarifications, we are not aware if they have the physical or financial resources to meet this responsibility.

In terms of the HAVA mandated review of the VSS to be performed by the EAC and NIST, we offer the following suggestions for greater guidance in the standards:

- Coding flaws – These may have security implications, such as vulnerable constructs. Some languages and their supporting libraries provide security vulnerabilities within their functions. This can allow for a buffer overflow (which is addressed in the VSS Volume 2 Section 5.4.2.d *"For those languages with unbound arrays, provides controls to prevent writing beyond the array, string, or buffer boundaries"*) or a stack overflow attack. Additional, and potentially more harmful, is the vulnerability to access the wrong program or data file. This makes the program susceptible to the introduction of external malicious code. We suggest providing language specific prohibitions of vulnerable constructs. Currently these vulnerable constructs can be used in programs without malicious intent but it is difficult in a static review to detect the security implication with their use.
- Race conditions – Synchronization issues, such as race conditions, present security vulnerabilities. Automated code checking tools can detect the potential for this situation but typically detect a number of "false positives". We suggest guidance on the acceptability of race conditions within the code.
- Global Variables – These variables are recognized throughout the program and in some cases are used to store critical status information that a number of programs need and therefore provide a valuable service; however, their potential for error and abuse should discourage their use. We suggest guidance on when they can and cannot be used.

We would also suggest that the standards include the following:

- Code Review Requirements for the vendors to provide documentation identifying the known security weaknesses of the programming language(s) they used, and their process for mitigating those weaknesses.
- Requirements for the vendors to provide documentation of their security practices. The standards need to also provide the ITAs with guidance for the review of this documentation to assure that security is incorporated into the vendor's development process.

Observations and Recommendations for NASED ITA Qualification Testing

The greatest challenge for NASED ITA Qualification Testing is the lack of understanding of what it is, what it is supposed to do, what it does not do and the role it should play in the entire election process.

What is NASED ITA Qualification Testing? It is the second of four levels of testing identified in the VSS.

- **Level 1 Vendor Testing:** The vendor tests to ensure that their system meets their design specifications, the requirements of the VSS, and any specifically supported state requirements.
- **Level 2 NASED ITA Qualification Testing:** The vendor's testing is reviewed for adequacy and additional testing is performed by software and hardware ITAs to ensure that the voting system meets the requirements of the VSS, and any additional functionality supported by the voting system as defined in the vendor's design specifications performs as specified.

- **Level 3 State Certification Testing**: State personnel or contractors perform testing under the direction of the state to ensure that the voting system meets *all* of the state's requirements.
- **Level 4 Acceptance Testing** Individual jurisdictions perform testing prior to each primary or general election to ensure that the voting system operates as required.

What is the objective of NASED ITA Qualification Testing? The intent of qualification testing is to ensure that only voting systems that pass independent testing to the minimum requirements of the 2002 FEC Voting System Standards are issued a NASED Qualification Numbers. This means

- The elements of the voting system (hardware, software, any required materials, and all documentation) have been defined, reviewed and tested for conformance with the requirements of the VSS;
- The voting system contains a method to successfully create elections, provide a ballot, record votes, provide report tallies, and produce an audit trail;
- Using the vendor's documented procedures and mandatory security processes, ensuring that voting is performed in a secret, accurate, reliable and secure manner;
- The source code has been reviewed and meets the requirements for modularity, maintainability, consistency, security, integrity, and the use of error handling;
- The code is sufficiently well commented so if the vendor cease to support the code it can be reasonably maintained by another entity;
- The code installed on the voting system for testing was built from the source code reviewed by an ITA and witnessed by an ITA;
- The Vendor's documents required by the VSS the requirements for content and format;
- The Vendor documentation required to assist the states and jurisdiction to configure, use and maintain the voting system (hardware, software, other required materials and documents) is accurate and sufficient to perform all supported functions;
- Security has been achieved through the demonstration of technical capabilities in conjunction with the documented mandatory administrative procedures for effective system security;
- Vendors have an established set of quality procedures and have supplied evidence of their implementation through development, internal testing, and ITA testing;
- The elements of the voting system configuration have been identified, tested and tracked by the ITA;
- Upon completion of testing a report has been issued to the NASED Technical Committee for peer review;
- The report has been accepted and retained by the NASED Technical Committee/EAC, the vendor and the ITA.
- NASED issued a qualification number.

What NASED ITA Qualification Testing does not mean:

- It does not mean that testing has been sufficient to confirm a voting system meets the specific laws of all the states or for that matter any state. There is much election functionality in the VSS that is optional. The VSS only requires that this work in terms of the vendor's own requirements for a function. Taking an example to the extreme, the VSS does not require a vendor to support primary or general elections; these are both optional functions. A vendor must support some sort of election, but the VSS allows the vendor to specify exactly what they choose to support.
- It does not mean that the code the vendor delivers installed on the voting system is exactly the code that was qualified. It does not mean that the hardware that was delivered by the vendor matches the

qualified hardware specification. While a version number may be the same, without a verification methodology at the state and local level, it is possible for unqualified versions to be used in an election.
- While security risks are significantly reduced, it does not mean that the voting system does not require an external audit process by the local jurisdiction for detection and prevention of irregularities. The same stringent audit processes jurisdictions apply should include the voting system.

What role should NASED ITA Qualification Testing play in the election process?
If one goes back to the implementation program for the 1990 Voting System Standards, one will see the direction that was originally intended. Qualification testing was just the first step. Additional phases were planned for state certification and local acceptance testing. There was a structure outlined for the accreditation of labs by NVLAP/NIST. The FEC was supposed to be a clearinghouse to make the reports available to state and local officials. Additionally, the states and local jurisdictions were encouraged to report their certification and acceptance testing to the clearinghouse. Escrow agents were envisioned to hold qualified versions of the code and assist the states and local jurisdictions in validation of qualified versions of code.

For unknown reasons, the later phases were not implemented. NASED assumed the role for accreditation. No official clearinghouse or escrow was established. States and local jurisdictions moved forward independently. NASED informally provided a meeting place to exchange information. The job of holding the report and source code fell to the NASED ITAs. As the vendors and the ITAs had non-disclosure agreements, delivery of the report beyond the NASED Technical Committee was at the request of the vendor.

While the vendor controls delivery of the report, it does not mean state and local officials do not have the right to see the report. The report is only confidential if the state certification or a local purchaser allows it to be a confidential. We receive instructions from the vendors to send their reports to state agencies.

We would suggest that in going forward:
- The 1990 Implementation Plan shall be used as guidance in completing the future structure of the qualification, certification and acceptance testing of voting systems. Whatever structure is implemented, it must minimally address the functions outlined in this baseline plan;
- A risk and needs assessment be performed against the roles outlined in the 1990 Implementation Plan to identify the capabilities of the players to understand and perform their roles;
- The needs of the state certification and local jurisdictions for using, understanding and interpreting the qualification report should be incorporated into the new standards from the EAC. The standards should define any specific reporting methodology to assist the states and local jurisdiction in understanding the reports;
- An annually updated, centralized database of all state specific voting requirements shall be made available to the ITAs, vendors, and election officials.